

Pět pravidel pro vaši bezpečnost

1 JAK ZACHÁZET S HESLEM

Přístupové heslo chrání informace o vašem projektu, které v systému MS2014+ zpracováváte. Každý, kdo zná vaše přístupové heslo, může provádět bez vašeho vědomí v systému činnosti stejně, jako byste je dělal vy. Proto musíte při výběru a použití hesla dodržovat bezpečnostní pravidla:

- a) udržovat heslo v tajnosti,
- b) měnit heslo v pokaždé, kdy mohlo dojít ke kompromitaci hesla,
- c) používat kvalitní hesla o postačující minimální délce, která mají následující vlastnosti:
 - nejsou založena na skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních informací, např. jméno, telefonní číslo, datum narození apod., nejsou napadnutelná útokem podle slovníku (tj. neskládají se ze slov obsažených ve slovníku),
 - neobsahují postupně po sobě jdoucí nebo stejné alfanumerické znaky,
- d) měnit heslo v pravidelných intervalech,
- e) nezačleňovat hesla do jakýchkoliv automatizovaných přihlášení, např. uložená v makru nebo pod funkční klávesou,
- f) nesdílet s nikým individuálně přidělená hesla, (pokud mimo vás se systémem pracuje i jiná osoba, měla by mít vlastní přihlašovací údaje a heslo)
- g) při přihlašování je uživatel povinen věnovat zadání hesla pozornost. Časté zadávání nesprávného hesla může vést k podezření na bezpečnostní incident.


2 POUŽÍVEJTE SILNÁ HESLA

Používejte silná hesla (tj. taková, která nelze je snadno uhádnout). Doporučujeme vám dodržovat při jejich vytváření následující pravidla:

- a) minimální délka hesla je 12 znaků,
- b) při tvorbě hesla povinně použít:
 - alespoň jedno malé písmeno (a-z), doporučuje se neužívat znaky „y“ a „z“,
 - alespoň jedno velké písmeno (A-Z), Doporučuje se neužívat znaky „Y“ a „Z“,
 - alespoň jednu číslici (0-9),
- c) nevytvářet jednoduchá hesla typu 12345Ab, Abcdef1,
- d) heslem nesmí být jméno nebo příjmení uživatele a také jméno uživatelského účtu uživatele, jména rodinných příslušníků, jména měst, jména známých osobností a další známá jména,

3 NEŽ ODEJDETE, ZAJISTĚTE SVŮJ POČÍTAČ

Pokud jste přihlášení k systému MS2014+ a potřebujete odejít od počítače, odhlaste se od systému MS2014+ před tím, než odjedete od počítače.

Pokud nechcete počítač vypnout, můžete jej před odchodem uzamknout pomocí zámku (ctrl+alt+del nebo +L), příp. jiným rovnocenným opatřením, např. spořičem obrazovky s heslem.

4 POUŽÍVEJTE ANTIVIROVÝ SW

Antivirová ochrana je jedním z bezpečnostních mechanismů, které snižují riziko infiltrace systému virem či jiným škodlivým kódem.

- Mějte na svém počítači antivirový program a pravidelně jej aktualizujte.
- Dávejte si pozor na spustitelné soubory pocházející z nedůvěryhodných zdrojů (nevyžádané e-maily, nedůvěryhodné WWW stránky, reklamní či soutěžní CD apod.).
- Proveďte antivirovou kontrolu každého média při jeho vložení do mechaniky, ještě před použitím na něm uložených dat.

5 ZÁLOHOVÁNÍ

Počítač je jenom stroj, který se může porouchat. Proto si svá důležitá data pravidelně zálohujte na výměnné médium (např. na Flash disk).